



**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES**

Attorney Docket No.: UK9-99-055

In re Application of:

SHAUN CARL KERIGAN

Serial No.: 09/315,656

Filed: May 20, 1999

**For: TRANSFER OF DVD DECODE
KEY ON A WINDOW BY
WINDOW BASIS TO AN
ATTACHED DEVICE**

Examiner: J. JACKSON

Art Unit: 2131

APPEAL BRIEF UNDER 37 C.F.R. §1.192

Mail Stop Appeal Briefs - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

RECEIVED
JUN 04 2004
GROUP 3600

Sir:

This Brief is submitted in triplicate in support of the Appeal in the above-identified application. A Notice of Appeal was filed in this case on March 23, 2004 and received in the patent office on March 26, 2004.

CERTIFICATE OF MAILING 37 CFR 1.8(A)

I hereby certify that this Appeal Brief is being deposited with the United States Postal Service via First Class Mail in an envelope addressed to Mail Stop Appeal Brief-Patents, Commissioner of Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Pia Lorenzana

May 25, 2004
Date

REAL PARTY IN INTEREST

The real party in interest in the present Appeal is International Business Machines Corporation of Armonk, New York, the Assignee of the present application as evidenced by the Assignment set forth at reel 009984, frame 0113.

RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences known to Appellants, the Appellants' legal representative, or assignee, which directly affect or would be directly affected by or have a bearing on the Board's decision in the pending appeal.

STATUS OF CLAIMS

Claims 1-12 have been canceled and claims 13-22 stand finally rejected as noted in the Examiner's action dated December 29, 2003.

STATUS OF AMENDMENTS

Claims 1-12 were canceled in Applicant's Amendment B submitted originally on March 26, 2004.

SUMMARY OF THE INVENTION

As set forth in the present specification at page 4, line 6 *et seq.*, the present invention provides an apparatus for processing an encrypted data stream within a computer system adapted to receive the encrypted data stream from a data storage device. The apparatus includes a data output device coupled to the computer system having a plurality of data output areas, means for transferring the encrypted data stream from the data storage device to the data output device wherein the encrypted data stream is output for one of the plurality of data output areas. Decryption means are provided associated with the data output device for receiving the encrypted data stream and for decrypting the encrypted data stream to produce a clear data stream for output to one of the plurality of data output areas wherein the decryption means receives a decryption key from the computer system relating only to encrypted data to be associated with a particular one of the plurality of output areas.

Thus, the present invention is directed to a technique for providing for display of a video signal in a manner which prevents the interception of an unencrypted video stream before the video stream is coupled to the display device.

As illustrated in Figure 2 and as described in the present specification at page 9, line 21 *et seq.*, a typical screen image 200 of a computer is shown as it appears on a display device 138. Screen image 200 includes a background 204 with data which is not in a DVD format and is not encoded appearing in a window 202. Background 204 and this data are correctly displayed in window 202 regardless of whether any DVD decode keys have been transmitted from the computing system 100 to the display 138 or not. Screen image 200 also contains two windows 206 and 208 which display DVD data. The data in these windows 206 and 208 is not displayed unless correct DVD decode keys for each window 206 and 208 have been transmitted from the computing system to display 138. Each window 206 and 208 has a separate key and data may be displayed in one window 206 but not the other window 208 in the event the key for window 206 is received but the key for window 208 is not received. A fresh key is sent for each frame of the displayed image.

This is further illustrated in Figure 3 and described in the present specification at page 10, line 12 *et seq.* As illustrated in Figure 3 a DVD disk data decode key is graphically illustrated which contains a 4-bit number of DVD windows presently displayed on display 138. The second field in the DVD disk data decode key contains the 64-bit DES key utilized to decode the DVD data. The third field contains the 16-bit X pixel start address and the 16-bit Y pixel start address of the window. The fourth field contains the 16-bit X pixel length, giving the size in the X dimension of the DVD window. The fifth field contains the 16-bit Y pixel length giving the size in the Y dimension of the DVD window.

Thereafter, as illustrated in Figure 4 and as described in the present specification at page 11, line 3, *et seq.*, display 138 incorporates a decoder 441 and decompressor 442 which receives encrypted DVD data from the interface 140. The decoder/decompressor 142 also receives DVD decode keys for any windows to be displayed on the display in which encoded DVD data is to be displayed. X address counter 444 is clocked by each pixel clock recovered from digital decoder

441. Y address counter 445 is clocked by a recovered data good signal or horizontal synchronization signal from digital decoder 441.

In this manner those skilled in the art will appreciate that encoded display data can be coupled to a display device for display within a particular window within that display device and by including a decode key with each frame of data to be so displayed, the data can be decoded at the display device for display without subjecting the video data to possible interception as a result of being transferred to the display device in a decoded manner such as that utilized in the prior art.

ISSUES

1. Is the Examiner's rejection of claims 13-18 and 20-22 under 35 U.S.C. § 102(e) as being anticipated by *Pinder et al.*, U.S. Patent No. 6,105,134 well-founded?

2. Is the Examiner's rejection of claim 19 under 35 U.S.C. § 103(a) as being unpatentable over *Pinder et al.* well-founded?

GROUPING OF THE CLAIMS

For purposes of this Appeal, claims 13-22 stand or fall together as a single group.

ARGUMENT

Claim 13, an exemplar for the claims of the single group of claims in the present application, is directed to a method for processing an encrypted data stream within a computer system. The method recites the steps of receiving an encrypted data stream from a data storage device and thereafter transferring that encrypted data stream "from said data storage device to a data display device having a plurality of data display areas..." the method thereafter recites the receipt of a decryption key "in said data display device" wherein said decryption key relates "only to said encrypted data stream associated with one of said plurality of data display areas."

Thereafter, the method recites decrypting, “in said data display device” said encrypted data stream to produce a clear data stream for output to one of said plurality of data display areas.

Pinder et al. discloses a cable television system which provides conditional access to services or programs which are broadcast and received in a plurality of “set top units” which are described within *Pinder et al.* as being utilized to selectively decrypt the instances for display to system subscribers. *Pinder et al.* describes that keys utilized by these set top boxes for selective decryption may be public or private in nature and may be reassigned to provide a cable television system with security such that piracy concerns are minimized.

A general overview of *Pinder et al.* can be determined by a cursory review of Figure 1 which is described in the specification thereof at column 4, line 14, *et seq.* As described therein, encrypted instances of programs such as encrypted instance 105 are broadcast over transmission medium 112. The medium may be wireless or wired and is utilized to transmit encrypted instance 105 to a large number of set top boxes, each signified by reference numeral 113. As set forth at column 4, line 41, *et seq.*, each such set top box “is attached to a television set.” Set top box 113 is further described as having as its primary function a determination of whether or not encrypted instance 105 should be decrypted to produce decrypted instance 123. Thus, despite the failure of *Pinder et al.* to depict a television set or any other “data display device” it should be beyond cavil that decryption of the encrypted data stream takes place within set top box 113 and thereafter, the decrypted version of a particular program or instance is coupled to a data display device. Thus, a recording device interposed between set top box 113 and a data display device will be able to record an unencrypted version of a program, contrary to the stated intent within the specification of the present application.

In comparison, claim 13, the exemplar for the claims of this group, expressly recites transferring “said encrypted data stream from said data storage device to a data display device having a plurality of display areas...” and further to that the decryption key is received “in said data display device” so that the encrypted data stream may be decrypted within the data display device. Applicant urges the Board to consider that having failed totally to depict a data display device and further, having shown decryption occurring within a set top box rather than within the data display device, *Pinder et al.* cannot be said by any stretch of the imagination to anticipate, show or suggest the method of the present invention in which an encrypted data stream is

transferred from a data storage device to a data display device and thereafter decrypted within the data display device. In support of this position, Applicant urges the Board to consider that “data display device” is of term of art clearly indicating a device capable of providing a visual display and that further the data display device is illustrated in the present specification as a computer display device such as a cathode ray tube or the like.

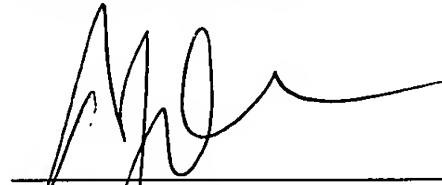
By performing decryption of an encrypted data stream within the display device rather than in a set top box or stand-alone decryptor such as that depicted within *Pinder et al.*, the method of the present invention prohibits the interposition of a recording device between the decrypting device and the display device where the unencrypted data stream might be recorded. In view of the above, Applicant urges that claims 13-22 define patentable subject matter over *Pinder et al.* and reversal of the Examiner’s rejections is respectfully requested.

Claim 19, separately rejected by the Examiner, recites that the plurality of data display areas within the data display device may include an area which is unencrypted and for which no decryption key is provided. The Examiner has urged rejection of this claim separately over *Pinder et al.* under 35 U.S.C. § 103(a) and Applicant urges, for the reasons set forth above, that this rejection is also not well –founded and should be reversed.

The Examiner has attempted to assert that a wide-spread cable television system having multiple subscribers, each subscriber having a television set clearly constitutes a data display device having a plurality of data display areas; however, this assertion fails to address the short fall of *Pinder et al.* in that it completely and absolutely fails to show or suggest in any way the decryption of an encrypted data stream within a data display device utilizing a decryption key which relates to an encrypted data stream associated with one of a plurality of data display areas within that data display device. Consequently, Applicant respectfully urges claims 13-22 define patentable subject matter and reversal of the Examiner’s rejection is respectfully requested.

Please charge the fee of \$330.00 for submission of a Brief in Support of Appeal to IBM Corporation Deposit Account No. 50-0563. No additional filing fee is believed to be necessary; however, in the event that any additional fee is required, please charge it to IBM Deposit Account Number 50-0563.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'AJD', written over a horizontal line.

Andrew J. Dillon
Reg. No. 29,634
DILLON & YUDELL LLP
8911 N. Capital of Texas Highway
Suite 2110
Austin, Texas 78759
512-343-6116

ATTORNEY FOR APPELLANT

APPENDIX

Claims 1-12: (canceled)

13. (previously presented) A method for processing an encrypted data stream within a computer system comprising the steps of:

receiving an encrypted data stream from a data storage device;

transferring said encrypted data stream from said data storage device to a data display device having a plurality of data display areas, said encrypted data stream being for output to one of said plurality of data display areas;

receiving a decryption key in said data display device, said decryption key relating only to said encrypted data stream associated with said one of said plurality of data display areas; and

decrypting, in said data display device, said encrypted data stream to produce a clear data stream for output to one of said plurality of data display areas.

14. (previously presented) A method according to claim 13 wherein said decryption key is received during an interval between transmission of successive images to said data display device and is protected by a suitable secure code.

15. (previously presented) A method according to claim 13 wherein said decryption key is received during an interval between transmission of successive lines of each image to said data display device and is protected by a suitable secure code.

16. (previously presented) A method according to claim 13 wherein:

data associated with the one of said plurality of data display areas is not displayed if the decryption key associated with the one of said plurality of data display areas is not received; and

data associated with others of said plurality of data display areas is displayed independent of the receipt or non-receipt of the decryption key associated with the one of said plurality of data display areas.

17. (previously presented) A method according to claim 16 wherein said data display device is a computer display and said data display areas are windows displayed on the display.

18. (previously presented) Apparatus according to claim 16 wherein data associated with one of said others of said plurality of data display areas is an encrypted data stream having a decryption key that differs from the decryption key associated with the encrypted data associated with the one of said plurality of data display areas.

19. (previously presented) A method according to claim 16 wherein data associated with others of said plurality of data display areas is an unencrypted data stream having no decryption key.

20. (previously presented) A method according to claim 16 wherein said decryption key contains an indication of the number of data display areas associated with the data display device which display encrypted data.

21. (previously presented) A method according to claim 16 wherein said decryption key contains an indication of the relative location of said data display area where said clear data stream is to be displayed.

22. (previously presented) A method according to claim 16 wherein said decryption key contains an indication of the size of said data output area where said clear data stream is to be displayed.